LAWFOYER INTERNATIONAL JOURNAL OF DOCTRINAL LEGAL RESEARCH

(ISSN: 2583-7753)

Volume 1 | Issue 4

2024

© 2024 LawFoyer International Journal of Doctrinal Legal Research

Follow this and additional research works at: www.lijdlr.com
Under the Platform of LawFoyer – www.lawfoyer.in

After careful consideration, the editorial board of LawFoyer International Journal of Doctrinal LegalResearch has decided to publish this submission as part of the publication.

In case of **any suggestions or complaints**, kindly contact info.lijdlr@gmail.com

To submit your Manuscript for Publication in the **LawFoyer International Journal of DoctrinalLegal Research,** To submit your Manuscript Click here

GENDER BASED VIOLENCE IN CYBERSPACE: A CRITICAL ANALYSIS OF LEGAL FRAMEWORK IN INDIA

Kanakshi Nema[1]

I. ABSTRACT

Gender-based violence (GBV) in cyberspace is a growing global concern and India is no exception to it. This paper explores the Indian legal framework for addressing this issue, based on data from an online survey conducted with cyber users. The paper starts by understanding the concept of GBV in cyberspace and its types including cyber stalking, online harassment and morphing. The important Indian cases related to the issue, stressing the difficulties victims face in getting justice are discussed. Furthermore, the research analyses the measures implemented by the Indian government to tackle GBV in cyberspace.

The paper contains findings from an online survey conducted, which highlights how ubiquitous GBV in cyberspace has become. The participants shared their perceptions, awareness and personal experiences, showing their concern on increasing number of instances of GBV in cyberspace. Further, the finding acknowledges that GBV affects individuals of all genders and not just females. These findings bring out the urgent need for addressing and preventing GBV in India, including more awareness, education, and stronger legislative measures. The paper identifies gaps in the existing legal system and concludes by proposing suggestions for bridging the gaps. It advocates for comprehensive legislation to address GBV, drawing attention to raise awareness and establish support mechanisms for victims, promoting access to justice.

II. KEYWORDS

[1] Student at Hidayatullah National Law University

© 2024. LawFoyer International Journal of Doctrinal Legal Research (ISSN: 2583-7753)

Gender-based violence (GBV), cyberspace, access to justice, public perception, Indian legal framework, online survey.

III. INTRODUCTION:

In the present era, technology for a modern man is what the fire used to be for the early man. It is omnipresent, blurring the boundaries between physical and virtual spaces i.e. cyberspace."Cyberspace" refers to a virtual and dynamic place, developed by the machine clones. It has opened up new avenues for communication, collaboration and commerce. However, it has also given rise to new forms of crime, including gender-based violence (hereinafter referred to as "GBV"). GBV is a global phenomenon that violates of human rights and affects health, self-respect, safety and individuality of victim. It is inherent in gender inequality and is predominantly inflicted against women and girls portraying patriarchal mindset of the society. However, there is no established definition. As a consequence of this, mostly "GBV" and "violence against women" are used as synonyms. With the advancement of technology, GBV is evident in virtual space with the same root cause and same impact on victim as in real world.

This research paper discusses about the intersection of GBV with cyberspace and its critical analysis of legal framework in India, with the help of responses collected through online survey of cyber users. The study shows that what is illegal offline is illegal online and frequently cybercrimes remains unreported because of lack of awareness about the legal mechanism in cyberspace. It aims to highlight the application of existing laws, its implementation in cyberspace, identify gaps and challenges in the implementation and make suggestions for a more comprehensive gender-based approach to cybercrime and development of more effective legal system to overcome present challenges.

IV. TYPES OF GBV IN CYBERSPACE:

Females are more susceptible to crimes from ancient times to this technological advanced world where violence is committed against them virtually. GBV in

cyberspaces includes various violence that abuse, threaten or harm individuals due to belonging to specific gender. Some of the cyber GBV are as follows:

- ***Cyber stalking:*** When internet and technology is used to harass or stalk another is cyberstalking[2]. It is considered more serious than cyberbullying and stalking in real world. The harassment, with the objective of retaliation, frustration or power, caused online by electronic communication devices, messaging, social networking platforms, and online discussion groups, etc. Different forms of cyberstalking include catfishing, keeping tabs on social network check-ins, spying using Google maps and Google Street View, stealing webcams, setting up stalkware, and using geotags to track position. Examples of cyberstalking includes false charges, defamation, slander and libel, surveillance, identity theft, vandalism, sex requests, or extraction of such data which can be deployed to harass, threaten or humiliate someone. A stalker can be a person whom the victim already knows or a stranger.
- ***Cyber Harassment:*** Cyber harassment differs from cyberstalking and involves unconsented and repetitive conducts like, threatening or harassing email/messages, or to post content online solely distressing an individual[3]. It further involves stalking, trolling, and sending threatening messages, with an aim to threat, injure, frustrate or dishonor a person by usage of digital technologies. It can be in the form of cyberbullying, cyberstalking, identity theft, doxxing, swatting, revenge porn, sextortion, etc. If the nature of cyber harassment is sexual where the harasser makes constant and unwanted sexual advancements is online sexual harassment.
- ***Cyber Defamation:*** It is a relatively new concept. It entails the act of posting misleading or defamatory information virtually against a person or organization.

[2] Fisher, B.S., F.T. Cullen, and M.G. Turner, Being pursued: Stalking victimization in a national study of college women. Criminology & Public Policy, 2002. 1(2): p. 257-308.
[3] The National Conference of State Legislatures (NCSL)

It is more grave than conventional concept of defamation as online world is more easily accessible, disseminates information in just few minutes with no geographical boundaries. It can seriously harm the victim's reputation and endanger their ability to maintain their health, livelihood, and financial security.

- ***Morphing:*** It literally means "to change the form or character of: transform."[4] In morphing face of an individual is changed with other person's body using technology. In other words, a special effect is given to motion pictures and animations in order to change an image or shape into another. The changes or alterations are seamless. Generally users download images and videos from different accessible online platforms, using morphing tools available online users alter the original content within few seconds and use such content against the victim to harm the victim. This cybercrime is rapidly spreading especially against females.

- ***Cyber Pornography:*** Britannica defines pornography as "representation of sexual behavior in books, pictures, statutes, motion pictures, and other media that is intended to cause sexual excitement."[5] It refers to publishing, disseminating or creating pornography or obscene material in cyberspace. People can view, download or upload pornographic content using their electronic devices easily. It includes sharing of intimate images and videos without consent of the person depicted seeking to injure him/her i.e. revenge porn.

- ***Cyber Flirting:*** In simple terms, cyber flirting means flirting on the internet or in cyberspace[6]. It is a petty offence. According to When the victim hears to obscene music, texts or any other content under the duress of the perpetrator, the offence of -cyber flirting is committed. It causes sexual defamation or the breach of trust.

[4] Merrian-Webster Dictionary
[5] https://www.britannica.com/topic/pornography
[6] https://www.yourdictionary.com/cyberflirting

- ***Email Spoofing:*** It is a kind of cyber attack or rather we can call it a fraud where emails messages are sent with a fake email address. This technique creates illusion to the user by making him believe that the email has been sent by some other known entity as similar fake headers are created so that user's device display fraudulent sender address, therefore it is used for spam and phishing attacks. When the user examines the header in detail, he is unable to realize the fraud. In cyberspace, the perpetrator collects personal data from females and uses them to blackmail them.

- ***Cyber Trolling:*** Trolling is when a person intentionally tries to threaten or directly attack anyone, by making derogatory comments through posting against him seditious, false and irrelevant or sending unconnected messages on online platforms to create trouble for the victim[7]. Trolls have huge negative impact as it is visible on all social platforms such as instagram, facebook, etc. It reduces both self esteem and social image of the victim.

- ***Hacking:*** It is the most common type of cybercrime. According to IBM, "Hacking (also called cyber hacking) is the use of unconventional or illicit means to gain unauthorized access to a digital device, computer system or computer network." It means unconsented access to computer system or network by identifying and abusing its weaknesses. It is a method used to gain unauthorised access to a private, public, corporate, or organization's computer network in order to obtain information. It is infringement of privacy. It is committed against females by taking control of her whole accounts and profile and modifying the content into disparaging.

- ***Cyber Bullying:*** It refers to "bullying that is done through the use of technology."[8] When the perpetrator intentionally or repeatedly tries to cause or causes injury to other person by the usage of digital technological advancements,

[7] https://dictionary.cambridge.org/dictionary/english/trolling
[8] Australian Human Rights Commission

cyber bullying is committed. It is a kind of bullying through transferring, uploading, or disseminating unfavourable, hurtful, or malicious content about another entity.

V. INDIAN LEGISLATIVE FRAMEWORK:

In India, there is no single piece of legislation dedicated to deal with GBV in cyberspace. Rather, the issue is addressed through combination of diverse. Some of these legislations are as follows:

1. *The Information Technology Act, 2000*[9]*:*

   The Parliament realized the need to recognize electronic transactions and activities. The Act provides enact strict regulations against cybercrimes, therefore various new provisions were added in 2008[10]. Chapter XI of the Act deals with "Offences", which talks about various punishments for cyber crimes including life imprisonment and fine upto rupees ten lakhs. Some of the important provisions of the Act are as follows:

   - "Section 65" reads as "tampering with computer source documents".
   - "Section 66" after Amendment Act, 2009 deals with "hacking with computer system" i.e. computer related offences.
   - "Section 66C[11] identifies identity theft and makes usage of another entity's password or e-sign a punishable offence.
   - "Section 66E[12]" prescribes "punishment for violation of privacy" i.e. for intentionally capturing, publishing or transmitting private pictures without consent.

[9]ACT NO. 21 OF 2000
[10]Information Technology (Amendment) Act, 2008 (Act 10 of 2009)
[11] Supra 9
[12] Supra 9

- "Section 67" prohibits publication, transmission or causing to be published or transmitted any obscene content in electronic form.
- "Section 67A[13]" lays down punishment for publishing, transmitting or causing of transmission of content like sexually explicit material.
- "Section 72" deals with "breach of confidentiality and privacy"

2. *The Indian Penal Code, 1860 (IPC)[14]:*

The IPC is a conventional statute, not specifically dealing offences in cyberspace. The Act was amended in 2013 for introducing provisions to directly deal with offences in cyberspace under section 354A to 354D. Provisions applying to GBV in cyberspace are as follows:

- "Section 292" penalizes sale or exhibition of obscene material and is extension of "Section 67 of the IT Act."
- "Section 509" deals with punishment for "word, gesture or act intended to insult the modesty of a woman".
- "Section 354A"[15] applies to sexual harassment in cyberspace.
- "Section 354C"[16] defines and penalizes "Voyeurism" as capturing or disseminating photographs of woman engaged in such circumstances in which she would "usually expect not to be seen, either by the offender of by anyone else acting at the perpetrator's direction".
- "Section 354D[17]"includes cyber stalking and penalizes the accused when he keeps an eye on the usage of the internet or on any communication done in electronic mode by a woman.

[13] Supra 9
[14] ACT NO. 45 OF 1860
[15] Inserted by 2013 Amendment Act
[16] Supra 14
[17] Supra 14

3. *Protection of Women from Domestic Violence Act, 2005*[18]*:*

When violence in cyberspace happens against a woman related to domestic relationships can be brought under this Act.

VI. EVOLUTION OF JUDICIAL APPROACH: ASSESSING KEY CASES:

Innovation comes along with its own unique challenges and so thus the technology. The Judiciary played vital role in interpreting and implementing the existing age old laws to address legal and philosophical issues in the cyberspace. Following are few landmark cases that establish jurisprudence in this domain:

- ***State (cyber cell) v Yogesh Pandurang Prabhu***[19]***:*** In this case, the accused was held liable for the offence of cyber stalking on the compliant of cyber cell under section 509 of the IPC read with Section 66E of the IT Act. This case was the first of this type where the victim made complaint to the cyber cell and accused was held guilty on that complaint of cyber cell. The decision recognized cyber cells as legitimate body to simplify reporting and prosecution of offence of cyberstalking, thus ensuring access to justice.
- ***Suhas Katti v. State of T.N.***[20]***:*** The first case of conviction under the IT Act for pornography convicted under "Sections 469 and 509 of the IPC" and "Section 67 of the IT Act". The victim rejected marriage proposal of accused. Thereafter accused harassed the victim by creating fake e-mail using her personal details and making them public. Thus, this created various problems for the victim and she lodged a case against the accused.

[18]ACT NO. 43 OF 2005
[19]C.C. No. 3700686/PS/2009
[20]C No. 4680 of 2004

- ***Avnish Bajaj v. State*[21]*:*** The Supreme Court declared that intermediaries are nonetheless liable for their actions in cyberspace and cited the necessity for legislation to stop the spread of pornographic materials online.
- ***Shreya Singhal v. Union of India*[22]*:*** A petition challenging the constitutionality of Section 66A was challenged on ground that this provision vague and restricts the freedom of speech in cyberspace. The Apex Court declared this section 66A as unconstitutional and recognized significance of free speech on the internet. This decision ensures a balance between addressing online harms and protecting fundamental rights.
- ***Sakshi v. Union of India*[23]*:*** The guidelines were laid by the Delhi High Court to tackle cyber harassment and revenge porn. Law enforcement agencies were also directed to take cybercrimes more seriously and social media platforms were ordered to cooperate during investigation.

These cases reflect the evolving and expanding approach of judiciary while addressing GBV in cyberspace. This shift is an example of the constant effort to establish a free and secure online space for everyone, especially for women who are more susceptible to abuse based on their gender.

VII. INTERNATIONAL LEGAL FRAMEWORK:

Cyberspace has no geographical borders and restrictions. It provides a platform which is accessible from anywhere across the globe. This makes the analysis of international legal framework for GBV in cyberspace of extreme significance. Following are some important relevant international instruments and framework related to this issue:

- **Universal Declaration of Human Rights (UDHR):** This document lays down basis of human rights. It includes freedom of speech and expression, right to

[21](2008) 105 DRJ 721: (2008) 150 DLT 769
[22]AIR 2015 SC 1523; Writ Petition (Criminal) No. 167 OF 2012
[23](2004) 5 SCC 546, AIR 2000 SC 3479

equality, protection from discrimination and violence, right to privacy. The scope of these principles extends to online activities and protects women's rights online by addressing violence against women in cyberspace.

- **Convention on the Elimination of All Forms of Discrimination against Women (CEDAW):** It talks about discrimination against women in all phases of life, including gender-based violence. Its scope extends to cyberspace in order to protect women's rights online and to combat violence against women.
- **Beijing Declaration and Platform for Action:** The declaration acknowledges the role of women's participation in all fields, including access to and use of information and communication technologies (ICTs). It also addresses violence against women including in cyberspace.
- **The United Nations General Assembly Resolutions on Women, Peace and Security:** The resolution deals with specifically gender related issues, including gender-based violence in cyberspace.
- **Internet Governance Forum (IGF):** It is a forum created under the United Nations with objective to engage people from diverse interest groups in discussions about Internet public policy issues on an equal basis including online safety and gender issues in cyberspace.
- **United Nations Sustainable Development Goals (SDGs):** Goal 5 of SDG is "gender equality" to provide women equitable access to the internet, technology, and sexual and reproductive health. It also aims "to reduce trafficking, sexual exploitation, and all other forms of violence against women and girls in both the public and private domains."
- **Regional Initiatives:** Various regional organizations have created their own regulations to combat cybercrimes against women.

One such regional initiative has been taken by the **Council of Europe** by entering into the **Istanbul[24] and Budapest Conventions[25]**, due to increasing cybercrimes targeting women. Istanbul convention recognizes online abuse as violence, requiring criminalization and victim support. Further, Budapest Convention lays down substantive and procedural laws on cybercrime, but does not specifically deals with gender based cybercrimes. Together, these conventions promote international cooperation and education to address this global issue, ensuring gender equality and safer online space. Other than the above-mentioned initiatives, UN General Assembly has also adopted various resolutions to raise concern about this issue. Resolutions of the 77th session, 2023 does not directly deal with gender equality rather recognizes the disproportionate impact of environmental degradation on women and girls, which can intersect with online harms. [26]

VIII. IMPACT OF EMERGING TECHNOLOGIES:

Technology is emerging like development of metaverse and other emerging digital spaces are prone to impact gender-based violence in cyberspace in both positive and negative ways.

Positive Impact: These technologies can be used to educate users to promote respectful online behavior, to provide them assistance and to improve reporting mechanisms for cybercrimes. It will make the reporting mechanism quicker and effective. Users frequently create self-policing organizations in virtual communities within the metaverse to defend one another. Women who face violence against them in virtual space could benefit from this by having a supportive atmosphere that encourages them to get assistance and report cases. Further, technological advancements have better

[24] The Council of Europe Convention on Preventing and Combating Violence Against Women and Domestic Violence known as the Istanbul Convention (2011)
[25] The Convention on Cybercrime, known as the Budapest Convention on Cybercrime (2001)
[26] Declaration of Access to a Clean, Healthy and Sustainable Environment as a Universal Human Right (A/RES/77/176, July 28, 2023)

security of communication and transactions and thus capable of reducing risk of few cybercrimes.

Negative Impact: A new technology comes with new challenges such as anonymity and pseudonymity, new types of cybercrimes, privacy concerns. When we specifically talk about metaverse, it contributes to increase anonymity issue by allowing users to create their avatar or use pseudonyms (fake names used for special purposes). This may promote perpetrators to commit crime in metaverse. This shows that how new forms of cybercrimes are being committed. In-game harassment and abuse directed towards women in e-sports is a problem that can lead to real-world cybercrimes. Recently, a 43 year old woman in the U.K. claims that she was raped "virtually" in metaverse within one hour of being in the metaverse.[27] Privacy issues like unauthorized recording, tracking, or sharing of personal information and experiences in virtual places may pose a risk to women.

IX. MEASURES TAKEN BY THE INDIAN GOVERNMENT:

Following are some measures taken by the central government to address GBV in cyberspace:

- **Cyber Crime Prevention against Women & Children scheme:** "Ministry of Home Affairs" provides financial assistance to all the States & UTs with aim to promote them "to develop cyber forensic-cum-training laboratories, training and hiring junior cyber consultants".
- **Campaigns for public awareness:** The government along with other non-governmental stakeholders has begun public awareness campaigns to inform people about safe internet usage, the significance of reporting cybercrimes, available cyber forensic technology and the legal remedies available to victims. The Ministry of Electronics and Information Technology (MeitY) conducts

[27] https://www.indiatoday.in/world/story/british-woman-virtual-gang-rape-facebook-metaverse-1908629-2022-02-04 (Last visited on 01 Jan 2024)

initiatives aimed at raising awareness of information security. For children, parents, and general users, information security-focused books, movies, and online tools are made.

- **National Cyber Crime Reporting Portal:** It is an initiative of the central government to help victims of cybercrime, specially children and women, to report a complaint online to make the procedure simple for the victims and promote reporting of cybercrimes. This portal is developed to report all types of complaints with an emphasis on crimes against women and children in particular.
- **Indian Cybercrime Coordination Centre (I4C):** It is 2018 government initiative, focusing on issues concerning cybercrime for citizens. It brings together different government agencies like the Central Bureau of Investigation, the National Investigation Agency, the Indian Computer Emergency Response Team, etc., providing a mechanism to ensure expertise and best practices in investigation of cybercrimes and digital forensics.
- **National Cyber Security Strategy:** This report was prepared established by the Data Security Council of India (DSCI) in 2020, focusing on 21 different areas to ensure cyber security in India. It also focused on ensuring cyber security for individuals to make social media sites safer.
- **Training Personnel:** Programs are being conducted to train enforcement personnel to improve their capacity for combating cybercrimes, particularly those involving GBV.
- **Assistance for Victims Services:** Many state governments provide counseling and mobile helpline services for victims of cybercrime committed against females. One such example is establishment of State Commission for Women in each state to provide counseling and support in lodging the complaint.

X. ASSESSING PUBLIC PERCEPTION AND AWARENESS: A SURVEY ON GBV IN CYBERSPACE:

The study seeks to analyze public perception and their experiences of GBV in cyberspace and also to examine their opinions on the existing legal framework of India in resolving this intricate and dynamic situation. An online survey was conducted, receiving 115 responses from regular cyber users. The majority of participants (72) fall within the 18-24 age group, with the remaining 25-34 years old. Gender distribution shows 60 females and 55 males, indicating a higher representation of young female participants.

The responses showed that majority of users (53) spend 2 to 4 hours on internet daily, suggesting the growing importance of the internet in daily life.

When questioned about their awareness GBV in cyberspace, 104 participants were aware, while 11 remained unaware despite spending significant time online. Further, 109 participants believe that GBV can be as serious in cyberspace as in physical spaces. One participant shared her experience as: "The incident of cyber stalking has impacted my regular life, developed fear for using social media. It has similar impacts as stalking in the physical world," indicating the graveness of the issue.

Out of 115 participants, majority (91) witnessed or experienced GBV in cyberspace, with 79 of them agreeing that such incidents have negative emotional impact on victims.

Participants also shared specific incidents they had witnessed or experienced. One participant described how someone created a fake Instagram profile using his sister's photo and initiated conversations with others while pretending to be her. Another participant recalled an incident where identity theft was committed by using the victim's pictures and details to engage in inappropriate conversations, leading to defamation and potential harm. Unfortunately, social stigmas often discourage victims from reporting such incidents.

Cyber violence affects victims' well-being. One participant mentioned deleting her profiles from all social media platforms after experiencing cyber stalking by a school friend; consequently she isolated herself from others. Tragically, one participant reported that her friend committed suicide, when she did not receive family support in reporting a cybercrime of sharing her explicit photos by ex-boyfriend

During the survey, it became evident that threats of revenge through online platforms had become a weapon often used against women. A participant shared that when she refused to talk to a stranger on social media, she received threats of sharing her forged photographs on a porn website. Another female participant discovered that the perpetrator had created a clone of her WhatsApp account, thereby gaining access to her messages, personal photos and location. Fearing the release of this sensitive information, she reported the incident to the Crime Branch. However, she faced ongoing threats and ultimately had to change her mobile phone and contact number.

The responses show that more than 50% of cases go unreported to the authorities. Participants cited several reasons for not reporting, including the stigma attached to such incidents (42%), lack of family support (35%), fear of societal judgment (30%), perceived ineffectiveness of authorities (24%) and the time and cost involved in reporting (20%). A significant portion of respondents (56) expressed hesitance to report future cybercrime incidents against any gender.

Out of 115 participants, only 44 were aware about India’s legal framework addressing GBV in cyberspace and 60 people believed that the existing legal framework in India is insufficient. Further , 94 participants expressed the view that the current legal mechanism is ineffective in preventing and addressing this issue and more stringent measures are required to combat such violence. Most participants who had reported incidents to the authorities found the present measures lacking in effectiveness. Challenges within the current legal framework include time-consuming processes, a lack of technical knowledge and infrastructure among authorities, obstacles in online investigations, difficulties in proving and tracking cybercrimes, low awareness about

the concept and reporting mechanisms, the under-recognition of emotional well-being impact and issues with online First Information Reports (FIRs). A 24-year-old male participant aptly summarized the challenges, stating, "The challenges are threefold: firstly, the legal framework is well designed but lacks stringent enforcement. Secondly, awareness about cyber abuse is lacking. Lastly, technology is advancing rapidly, necessitating legal evolution to keep up with cybercriminals."

Regarding awareness, 86 participants believed that there is a need for more awareness and education about GBV in cyberspace in India. Additionally, 77 participants were unaware of support services and resources available for victims of GBV in cyberspace in India. Participants proposed several suggestions to raise awareness and promote education on this issue, including training for law enforcement personnel, educational campaigns or workshops in schools and colleges, inclusion of relevant content in the curriculum, engagement of social media platforms in awareness efforts, regulatory bodies for content review in cyberspace, promotion of safe online practices, mandatory advertising on social media platforms, public awareness programs and consultations with intermediaries and public participation to enforce regulations.

These results highlight the crucial need to address and prevent GBV in cyberspace, not just via legal means but also through awareness campaigns, support networks and education.

XI. VIOLENCE AGAINST MEN AND THIRD GENDER IN CYBERSPACE:

When we say GBV, it is commonly understood as only crimes against women. Various provisions of the Indian legal system do not differentiate on the basis of gender or sex while prosecuting for cybercrimes. The IT Act and IPC is applicable universally on everyone irrespective of gender. However, language used in the laws are not gender-neutral, modernizing the language is required. Various cases remain unreported due to stigma and lack of awareness in reporting cases by male and third gender victims.

Awareness campaigns need to be conducted to overcome this issue. Male consent is not considered relevant and non consensual sharing of their images remains unreported and unaddressed. Law enforcement agencies take cybercrime against men and individuals of third gender for granted and therefore training should be imparted to them.

The online survey also acknowledged the fact that the term GBV signifies crimes committed against individuals based on their gender, whether male, female, or third gender. A male participant shared an incident where he met a girl through an online dating platform. After engaging in video calls, she blackmailed him by threatening to share explicit video footage unless he paid her. One more similar incident was shared by a participant. While such incidents are less common than those targeting women, women have also employed this tactic against men in cyberspace.

XII. SUGGESTIONS AND CONCLUSION:

Various loopholes can be traced when we examine the Indian legal system to combat GBV in cyberspace. Few of them are as follows along with suggestions based on analysis of survey and findings in the paper to fill the existing gaps:

- ***Comprehensive Legislation:*** There is no comprehensive legislation to address GBV in cyberspace. The IT Act uses the word "whoever", which covers both males and females i.e. provisions are general. There is no crime or punishment specifically incorporated for GBV in cyberspace. The gender-specific provisions incorporated by 2013 Amendment to the IPC are not sufficient to address the current issues. There is a need to legislate gender-specific provisions to make the laws more stringent and acknowledge the needs of the gender victims. It should use inclusive language to acknowledge and protect all genders equally along with their gender identities.
- ***Privacy and Consent related Issues:*** The IT Act and IPC have narrow scope, as they have confined privacy to physical body and not beyond that. However, the

Parliament has enacted the "Digital Personal Data Protection Act, 2023[28]," to protect personal data acquired or transformed in digital form. Also, consent is required to process any "sensitive personal data" and impact analysis of data protection to improve safety in cyberspace. However, the Act fails to regulate gender-specific issues. There is still need to create provisions regarding privacy and consent with special reference to GBV in cyberspace.

- ***Revenge Porn Laws:*** The Courts have recognized revenge porn as an alarming concern. But there is no specific provision to regulate cases related to revenge porn. Such cases are penalized under the provisions of the IPC, but these provisions fail to address the issue completely.
- ***Anonymity Issue:*** The Internet serves a challenge of non-disclosure of the real identity of an individual i.e. anonymity, eventually promoting crimes in cyberspace. A mechanism should be developed for identifying and tracking the accused in cyberspace with the help of online platform and service providers.
- ***Lack of Obligation on Intermediaries:*** The online platforms undermine the need to assess the non fulfillment of their user terms and conditions by the users, by disregarding the intermediary guidelines under the IT Act. Therefore, more stringent role for online platforms should be outlined to combat GBV in cyberspace to hold them liable. Additionally, law enforcement agencies can collaborate with tech companies to create and implement clear guidelines against abuse and harassment on the internet.
- ***Administering Electronic Evidence:*** Although the IT Act and the "Indian Evidence Act, 1872[29]" incorporate provisions related to evidence in electronic form, still challenges occur in addressing administration of electronic evidence.

[28] NO. 22 OF 2023
[29] ACT NO. 1 OF 1872

Therefore, better infrastructure and training should be provided to law enforcement personnel to handle electronic evidence effectively.

- ***No provisions related to Mental Health:*** The current legal framework places a strong emphasis on physical harm but leaves out mental harm. However, they must also take into account the psychological harm that victims endure throughout the procedure by establishing specialized therapy and legal assistance programs for victims.
- ***Awareness and Reporting:*** Due to fear of repercussions or social stigma attached to such crimes, incidents remain unreported. They are also unaware of legal recourse available. A user-friendly and private reporting channel should be created for cybercrime victims to make it simpler for people to come forward with happenings without worrying about repercussions.

Conclusion: In the digital era, information technology regulates every aspect of life, offering cost reduction and streamlined processes but has also introduces new forms of cybercrime, particularly against women. A society free from crime is not possible but still it is a dream, but legislators try to make safer environments. In the face of the growing prevalence of cybercrime, driven by emerging technologies and increased accessibility, exceptional measures are needed. Technology possesses the dual capacity for both constructive and destructive purposes.

This paper focused on gender-based differential treatment and critically assessed the existing legal framework in India for prosecuting GBV in cyberspace. While amendments have been made to incorporate provisions for regulating online GBV, the current legal landscape requires further modifications. Certain provisions remain vague during implementation. Given the ever-evolving nature of technology, laws must adapt to address new forms of wrongs committed using technology.

Survey findings shows combination of understanding and knowledge gaps among participants, demonstrating the need for greater awareness and education on this

crucial subject. It is more important to make sure people are aware of their rights and the legal remedies in incidents of online GBV. The survey results provide important information that can serve as a foundation for upcoming awareness campaigns, legislative reforms and other initiatives aimed at making a safer and more inclusive online environment. It is crucial for stakeholders, including legislators, advocacy organizations and educational institutions, to work together to raise awareness, promote digital literacy and develop the legal framework to prevent GBV in cyberspace to handle this issue successfully. In the digital age, this study represents a critical first step toward a more informed and empowered society. Ultimately, our hope is that this study can initiate discussions and contribute to the improvement of the digital realm, making the internet a safer space for all, regardless of gender. This goal is not only desirable but also need of the hour.

XIII. BIBLIOGRAPHY

Primary Sources: Legislations-

- The Information Technology Act, 2000
- The Indian Penal Code, 1860
- The Protection of Women from Domestic Violence Act, 2005
- Criminal Law (Amendment), Act 2013
- Digital Personal Data Protection Act, 2023

Secondary Sources:

- Association for Progressive Communications (APC). (2011). Voices from digital spaces: Technology-related violence against women. APC WNSP.

  https://www.apc.org/sites/default/files/APCWNSP_MDG3advocacypaper_full_2011_EN_0.pdf

- Ajaykumar, S. (2022). Gender-based violence in private online spaces. Observer Research Foundation. https://www.orfonline.org/expert-speak/gender-based-violence-in-private-online-spaces/
- United Nations Broadband Commission Working Group on Broadband and Gender. (2015). Cyber Violence against Women and Girls: A World-Wide Wake-Up Call. Broadband Commission for sustainable development.https://en.unesco.org/sites/default/files/genderreport2015final.pdf
- Government of India. (2016). National Policy for Women, 2016.https://wcd.nic.in/sites/default/files/draft%20national%20policy%20for%20women%202016_0.pdf
- Government of India. (2015). Digital India Initiative, 2015.https://www.meity.gov.in/sites/upload_files/dit/files/Digital%20India.pdf

Annexure:

The questionnaire for empirical research on **GBV in Cyberspace** is attached herein under:

1. What is your age range?
    a. Under 18
    b. 18-24
    c. 25-34
    d. 35 and above
2. Gender
    a. Male
    b. Female

c. Other

3. On average, how many hours per day do you spend online?
    a. Less than 1 hour
    b. 1-2 hours
    c. 2-4 hours
    d. More than 4 hours
4. Have you heard about gender-based violence occurring in online spaces?
    a. Yes
    b. No
5. Do you believe that gender-based violence can occur in cyberspace as seriously as in physical spaces?
    a. Yes
    b. No
6. Have you or someone you know ever witnessed or experienced any form of gender-based violence in cyberspace?

    (e.g., unwanted sexual comments, gender-based discriminatory memes and posts, threatening comments, hate speech, trolling, cyber stalking, sharing content without consent, hacking, identity theft, gender-based sexual abuse, cyberbullying, online harassment, revenge porn)
    a. Yes
    b. No
7. If yes, did the incident(s) impact your/their emotional well-being?
    a. Yes
    b. No

8. Briefly describe the incident(s) you witnessed or experienced:

   (optional)

9. Did you report it to the relevant authorities or platforms?
   a. Yes
   b. No
10. Are you aware of any legal provisions in India addressing gender-based violence in cyberspace?
   a. Yes
   b. No
   c. Maybe
11. Do you think the existing legal framework in India adequately addresses gender-based violence in cyberspace?
   a. Yes
   b. No
   c. Maybe
12. In your opinion, how effective are the existing legal measures in preventing and addressing gender-based violence in cyberspace in India?
   a. Very effective
   b. Somewhat effective
   c. Not very effective
   d. Ineffective
13. Do you think that more stringent measures by authorities are required for the accused and this will help in minimizing gender-based violence in cyberspace
   a. Yes

b. No

14. What challenges, if any, do you think exist in the current legal framework to combat gender-based violence in cyberspace?

(optional)

15. If you or someone you know experienced gender-based violence in cyberspace, would you feel comfortable reporting it to the authorities?

a. Yes

b. No

16. If no, why? [Checkbox]

a. Taboo/stereotype attached

b. Family won't support

c. Fear of the society

d. Belief that authorities are not that effective in delivering justice

e. Time and cost involved in reporting to authorities

f. Other…

17. Do you think there is a need for more awareness and education about gender-based violence in cyberspace in India?

a. Strongly agree

b. Agree

c. Neutral

d. Disagree

e. Strongly Disagree

18. Are you aware of support services and resources available for victims of gender-based violence in cyberspace in India?

a. Yes

b. No

19. Do you believe that legal regulations and awareness campaigns have contributed to a reduction in gender-based violence in cyberspace in India?

a. Yes

b. No

c. Maybe

20. How do you believe awareness and education about this issue could be improved?

(optional)